PENNSTATE

Jens Grossklags, Ph.D.
Haile Family Early Career Professor
Assistant Professor of Information Sciences and Technology
Director, Security, Privacy and Information Economics Laboratory (SPIEL)

The Pennsylvania State University
College of Information Sciences and Technology
329A IST Building
University Park, PA 16802
Phone: 814-867-4211
Email: jensg@ist.psu.edu

For: Submission of Research Paper for Participation in FTC PrivacyCon

Dear Organizers of the FTC PrivacyCon,

I herewith submit the forthcoming research article "*An Empirical Study of Web Vulnerability Discovery Ecosystems*" co-authored by Mingyi Zhao, Jens Grossklags, and Peng Liu, to be considered for a presentation and discussion at PrivacyCon. Our work has been rigorously peer-reviewed and will be presented at the 22nd ACM Conference on Computer and Communications Security (CCS 2015) to be held in October 2015 in Denver, Colorado. CCS is one of the most selective conferences in the field of computer and information security.

The goal of our study is to understand the trajectory, impact and dynamics of emerging web vulnerability discovery ecosystems based on two leading bug bounty platforms. We have collected publically available data from HackerOne (a US-based bug bounty platform) and Wooyun (a China-based vulnerability disclosure platform) and analyzed the data in a rigorous fashion.

Below I provide the required submission information as well as a partial overview of our analyses.

Name: Jens Grossklags

Email: jensg@ist.psu.edu

Office phone: 814-867-4211

Abstract:

In recent years, many organizations have established bounty programs that attract white hat hackers who contribute vulnerability reports of web systems. In this paper, we collect publicly available data of two representative web vulnerability discovery ecosystems (Wooyun and HackerOne) and study their characteristics, trajectory, and impact. We find that both ecosystems

include large and continuously growing white hat communities which have provided significant contributions to organizations from a wide range of business sectors. We also analyze vulnerability trends, response and resolve behaviors, and reward structures of participating organizations. Our analysis based on the HackerOne dataset reveals that a considerable number of organizations exhibit decreasing trends for reported web vulnerabilities. We further conduct a regression study which shows that monetary incentives have a significantly positive correlation with the number of vulnerabilities reported. Finally, we make recommendations aimed at increasing participation by white hats and organizations in such ecosystems.

Key analyses and findings:

- We observe an increasing number of active white hats per month and a constant flow of newcomers per month, leading to continuous expansion of the white hat community.
- We detail the individual and aggregate contributions of white hats who are most prolific and those who only rarely make contributions. We show that low productivity white hats nonetheless contribute a high number of severe vulnerabilities.
- We analyze how the white hat community learns from disclosed vulnerability reports.
- We provide evidence on which types of organizations are more likely to join bug bounty platforms.
- We explore in detail the behavior of organizations which receive vulnerability reports. On HackerOne, 75% of the disclosed reports are resolved in 25 days. On Wooyun, 23% of the reports have no response from the organizations, and smaller websites have a higher no-response rate and rely more on third parties (e.g., CNCERT).
- We carefully investigate the bounties paid by organizations for discovered vulnerabilities.
- We analyze the trend of discovered vulnerabilities over time, and how the security of organizations with a significant number of vulnerability reports is likely affected.
- We show that the size of the paid bounties and the size of the affected organizations are significantly correlated with the number of vulnerability reports received.

Methodology:

- Collection and analysis of publicly available data from two major web vulnerability disclosure platforms
- Dataset including 10000s of web vulnerability reports with information about the submitting white hats, severity types and other important factors

Novelty:

- Our CCS 2015 paper expands our own findings from a previous workshop publication. In the related work section of this submission, we describe in detail how our research expands on previous work.

We would welcome the opportunity to present our research at PrivacyCon. Thank you for considering our submission.

With best regards,
Jens Grossklags